PSIN 2023

Política da Segurança da Informação

SERPROS
FUNDO MULTIPATROCINADO

Sumário

SERPROS FUNDO MULTIPATROCINADO	**POLÍTICA**		
	Código: **SERPROS-DP-GETEC-POL-01**	**Versão:** **3.0**	**Página** **2 de 9**
Título: Política de Segurança da Informação			**Classificação:** **Pública**
Processo: **11. Gestão de Tecnologia da Informação**		**Área Emitente:** **Gerência de Tecnologia da Informação**	
Elaborador: **Flavio Fernandes de Oliveira** **Gerente de TI**	**Verificador:** **Diretoria Executiva**	**Aprovador:** **Conselho Deliberativo**	

1. HISTÓRICO DO DOCUMENTO

Este documento substitui a PSI 2020, adicionando as novas regras de controle de segurança apresentadas na **LGPD**.

Quadro de Artefatos

2. INTRODUÇÃO

Este documento tem o objetivo de estabelecer o direcionamento estratégico da Segurança da Informação e da Segurança Cibernética, em alinhamento com os requisitos de negócio, de forma a assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade dos serviços e sistemas de informação e dos recursos gerenciados pelo SERPROS.

3. OBJETIVOS

A PSI do SERPROS, tem os seguintes objetivos:

a) Definir o escopo de segurança da instituição;

b) Orientar, por meio de suas diretrizes, todas as ações de segurança, para reduzir riscos e garantir a integridade, confidencialidade e disponibilidade dos sistemas de informação e seus recursos;

c) Permitir a adoção de soluções de segurança integrada;

d) Servir de referência para auditoria, para apuração e avaliação de responsabilidades.

4. ABRANGÊNCIA

A PSI SERPROS abrange os seguintes aspectos de Segurança:

a) Humana;

b) Física;

c) Lógica;

5 TERMINOLOGIA

As regras e diretrizes de segurança são interpretadas de forma que todas as suas determinações são obrigatórias sem exceções.

6 CONCEITOS E DEFINIÇÕES

6.1 - **Ativo de Informação** – é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos do SERPROS;

6.2 - **Ativo de Processamento** – é o patrimônio composto por todos os elementos de Hardware e Software necessários para a execução dos sistemas e processos do SERPROS, tanto os produzidos internamente quando os adquiridos;

6.3 - **Direito e Controle de Acesso** – estão definidos na **Norma de Controle de Acesso Digital do SERPROS**;

6.4 - **Ferramentas** – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a PSI do SERPROS.

6.5 - **Política de Segurança** – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação do SERPROS;

6.6 - **Auditoria e Fiscalização** – Todos os Sistemas devem fornecer LOGs, para trilha de auditoria, sendo necessário disponibilizar Views (consultas) para a execução dos trabalhos de fiscalização.

6.7 - **Gerenciamento de Riscos** – Processo que visa a proteção dos serviços do SERPROS, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) viável.

6.8 - **Plano de Continuidade do Negócio** – Manter em funcionamento os serviços e processos críticos do SERPROS, na eventualidade da ocorrência de desastres, atentados, falhas e intempéries.

7 DIRETRIZES GERAIS

7.1 - A Política de Segurança do SERPROS se aplica a todos os seus recursos humanos, administrativos e tecnológicos. A abrangência dos recursos citados refere-se àqueles ligados a ela tanto em caráter permanente quanto temporário;

7.2 - Esta política é comunicada para todo o pessoal envolvido e largamente divulgada pelo SERPROS, garantindo que todos tenham consciência da mesma e a pratiquem na organização;

7.3 - Todo o pessoal deve receber as informações necessárias para cumprir adequadamente o que está determinado nesta política de segurança;

7.4 - Programa de Treinamento e Conscientização sobre segurança da informação foi implementado, conforme **Norma de Conscientização de Segurança da Informação**, para assegurar que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos.

7.5 - O registro de atividades relativas ao acesso e uso dos sistemas devem ser mantidos em repositório centralizado.

7.6 - Os processos de aquisição de bens e serviços, especialmente de Tecnologia da Informação – TI, devem estar em conformidade com esta Política de Segurança;

7.7 - Os riscos associados aos sistemas, serviços e ambientes do SERPROS, devem ser identificados, analisados e tratados constantemente.

7.8 - Todos os ativos do SERPROS devem ser inventariados, classificados, permanentemente atualizados, e possuir gestor responsável formalmente designado;

7.9 - O SERPROS implementou o **PCN** onde apresenta controles e execução de testes a cada 12 meses ou menos, para garantir a continuidade dos serviços críticos, sendo administrado pela área de Riscos e Compliance.

8 SEGURANÇA DO AMBIENTE LÓGICO

8.1 - Os dados, as informações e os sistemas de informação, são protegidos através dos controles:

- Usuário e senha
- Para usuários que executam atividades remotas é disponibilizada VPN de acesso
- Firewall gerenciado, que controla os acessos e disponibiliza apenas os sistemas, pastas e arquivos definidos anteriormente.

8.2 - As violações de segurança devem ser registradas e associadas no tratamento de incidentes.

8.3 - Os Bancos de Dados de todos os sistemas que são utilizados para processamento, armazenamento e transmissão dos ativos, devem estar registrados e mantidos atualizados.

8.4 - Os Ambientes (Desenvolvimento, Homologação) utilizados para suprir as áreas de desenvolvimento e validação de novas rotinas de TI, devem possuir os mesmos controles de acesso que o ambiente de Produção.

8.5 - As necessidades de segurança são identificadas para cada etapa do ciclo de vida dos sistemas. A documentação dos sistemas é mantida atualizada. A cópia de segurança é testada e mantida atualizada;

8.6 - Os sistemas possuem controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação da autorização está claramente definido e registrado;

8.7 - Os arquivos de logs estão criteriosamente definidos para permitir recuperação nas situações de falhas, auditoria nas situações de violações de segurança e contabilização do uso de recursos. Os logs são periodicamente analisados, gerando evidências de teste e apresentados nos controles do PCN;

8.8 - Os acessos lógicos, ao ambiente ou serviços disponíveis em servidores, são controlados e protegidos. As autorizações são revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização está claramente definido e registrado;

8.9 - São adotados procedimentos sistematizados para monitorar a segurança do ambiente operacional:

- Os eventos de acesso aos Bancos de Dados, são armazenados em arquivos de segurança (Logs), permitindo rastreabilidade e análise para auditoria.

- Os eventos de acesso aos Arquivos (Documentos e Imagens) são controlados através de acesso do usuário.
- Para melhorar os controles e executar a rastreabilidade, destes arquivos é necessário a implantação de ferramenta administrativa, onde é possível controlar todas as atividades de Leitura, Transmissão, cópia e exclusão.

8.10 - Qualquer apresentação (POC) ou aquisição de sistemas, para as áreas de negócios ou operacionais, devem ser comunicadas à área de TI, que deverá avaliar a solução e apresentar relatório de avaliação técnica.

8.11 - A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração são formalmente documentadas e mantidas, de forma a permitir registro histórico, tendo a autorização da administração da rede e da gerência de segurança. O diagrama topológico, a configuração e o inventário dos recursos são mantidos atualizados;
São adotadas proteções adicionais para os recursos de rede considerados críticos (Firewall);

8.12 - Todo serviço de rede não explicitamente autorizado será bloqueado ou desabilitado;

8.13 - Os registros de eventos são monitorados através de mecanismos sistêmicos e apresentados para os profissionais de TI, através de Painel de Controle e envio de mensagens de alerta;

8.14 - As ferramentas de detecção de intrusos são implantadas para monitorar as redes críticas, alertando periodicamente os administradores das redes sobre as tentativas de intrusão.

9 COMPUTAÇÃO PESSOAL

9.1 - São adotadas medidas de segurança lógica referentes a combate a vírus, backup, controle de acesso e uso de software não autorizado;

9.2 - Para atender este requisito é necessário que todos os documentos gerados ou atualizados sejam salvos nas Pastas dos servidores do SERPROS.

9.3 - As informações armazenadas em meios eletrônicos são protegidas contra danos, furtos ou roubos, sendo adotados procedimentos de backup, definidos no **Procedimento de Backup/Restore**; este procedimento só é efetivo quando os arquivos e documentos são salvos no Servidor.

9.4 - Todos os equipamentos utilizados devem ser configurados apenas com os Softwares homologados pela área de TI.

9.5 - Combate a Vírus de Computador

Os procedimentos de combate a malware são sistematizados e abrangem máquinas servidoras, estações de trabalho, equipamentos portáteis e microcomputadores stand-alone.

10. CLASSIFICAÇÕES DAS INFORMAÇÕES

A classificação das informações é parte integrante da Gestão da Segurança da Informação da Entidade e determina o nível que sua proteção possui quando tramitada interna ou externamente, estejam em meio físico ou eletrônico.

O Responsável pela emissão da informação deve determinar sua classificação, observando os critérios definidos na presente Política de Segurança da Informação, em observância aos requisitos legais, aos interesses institucionais, à proteção de dados pessoais e à segurança da informação, de forma a garantir a privacidade, integridade, confidencialidade, disponibilidade, autenticidade e legalidade.

As informações tratadas pela entidade devem ser classificadas como:

1. **Públicas**: aquelas cuja publicação ou divulgação para o público externo decorra de determinação legal ou do interesse do Serpros e que não afetem a governança corporativa ou os interesses dos participantes, assistidos, empregados e demais titulares de dados. Pode ser encaminhada em qualquer tempo, a qualquer público, pois trata-se de informação que não fere a integridade e a aplicação das estratégias adotadas pela Entidade, sendo sua publicação recomendável ou obrigatória.

2. **Restrita:** acesso apenas ao público interno da Entidade, podendo ser encaminhada aos órgãos fiscalizadores, auditorias e órgãos do governo quando solicitado formalmente.

3. **Confidencial:** acesso exclusivo às pessoas as quais foram atribuídas permissões específicas pelo responsável do documento.

Vide Norma de Classificação das Informações para maiores detalhes

11. DOCUMENTOS REFERENCIADOS

Os documentos apresentados abaixo são públicos.

Norma de Conscientização de Segurança da Informação
- Norma de Classificação das Informações
- Norma de Controle de Acesso Digital

12. APROVAÇÃO

Esta Política foi aprovada na 11ª Reunião Ordinária do Conselho Deliberativo em 30/08/2023, através da DL 038/2023, e vigora a partir de sua publicação.